Universidad de Los Andes
ISIS-2203 – Infraestructura Computacional

Daniela Jaimes – 201531521
David Narvaez – 201516897

Caso 2
Canales Seguros

Análisis y Entendimiento del Problema

1. Identifique y describa los datos que deben ser protegidos en el sistema de rastreo de unidades de distribución. Explique su respuesta en cada caso y responda la pregunta: Si un actor no autorizado consigue acceso al dato mencionado, ya sea en modo lectura o escritura, ¿cómo podría afectar la empresa?

   - **Origen:** La información de origen del paquete debe ser protegida dado que un tercero podría acceder a esta información. Si esto sucede, pueden suceder dos cosas:
     - **Escritura:** El interceptor puede utilizar esta información para evitar que el paquete se entregue en su destino, dado que, si lo cambia, lo hará parecer como un error de la empresa.
     - **Lectura:** O bien para conocer cuanto valor hay en una bodega con el fin de hurtar los paquetes que residen ahí.

   - **Destino:** La información de destino del paquete solo debería ser conocida por el servidor, el cliente que lo envía y el cliente que lo va a recibir dado que no se desea que un tercero pueda conocer a donde llegara el paquete. Esto ya que con esta información el tercero podría
     - **Escribir:** Hacerle alguna modificación o cambio al momento de su llegada o podría hacer que se pierda el paquete y jamás llegue a su destinatario.
     - **Leer:** Un tercero sabría información confidencial que solo debería conocer la empresa y los clientes involucrados en la transacción.

   - **Localización en tiempo real:** Es necesario que esta información esté restringida por lectura solamente para la empresa y el cliente y escritura solo por la unidad de transporte. En los peores escenarios pueden suceder los siguientes ataques:
     - **Escritura:** La ubicación de la unidad que transporta la mercancía es alterada con el fin de hurtar los paquetes de esta, esto hace que la empresa pierda credibilidad y clientes además de dinero
     - **Lectura:** Una persona foránea al caso de uso podría conocer la ubicación de la unidad con el fin de interceptarla y alterar sus productos o hurtarlos.

   Si cualquiera de estos datos se ve afectado, resultaría en que no se le estaría dando un servicio de calidad al cliente lo que podría generar una pérdida de clientes cosa que no sería beneficiosa para la empresa. Además, el paquete que se le estaría entregando al cliente sería uno corrupto lo cual presentaría consecuencias graves, incluso a la pérdida de este.

2. Identifique cuatro vulnerabilidades del mismo sistema, teniendo en cuenta únicamente aspectos técnicos o de procesos (no organizacionales). Identifique vulnerabilidades no solo en lo relacionado con la comunicación sino también con el almacenamiento y procesamiento de los datos. Explique su respuesta en cada caso.

   - **Vulnerabilidad sobre la red celular:** Dado que no hay una autenticación sobre quien hace las peticiones, puede existir el ataque conocido como "*man-in-the-middle"* en el cual un agente externo intercepta la comunicación y puede, ya sea, leer los datos o modificarlos sin que las partes se den por enteradas. Lo anterior puede causar modificación en las bases de datos, pérdida de información real o incluso infectando los servidores con scripts maliciosos que afecten la integridad de la información, de los componentes físicos o de la misma empresa a través de *exploits*.

   - **Vulnerabilidad en los datos almacenados:** Dado que todas las comunicaciones se realizan a través de red celular se puede presentar la situación de que no sea posible enviar la información y deba ser almacenada en el dispositivo móvil, lo que presenta problemas en términos de capacidad y seguridad. En términos de capacidad se puede presentar que si el celular utilizado no tiene suficiente almacenamiento y una alta cantidad de datos no puedan ser enviados la memoria del celular se llene en algún punto y se pierdan algunas tomas que pueden ser importantes. Para el área de seguridad si alguien logra acceder a esta información que esta almacenada antes de ser transmitida se podrían cambiar datos y generar una modificación no autorizada de datos o fraude y cuando se logre recomenzar la transmisión de información estos datos serian corruptos o si alguien logra leerla puede acceder a información confidencial, Robo de información y espionaje continuo. Ambas situaciones podrían llegar a afectar el proceso de la compañía.

   - **Suplantación:** De igual manera se puede dar una suplantación de identidad, dado que no hay una autenticación por parte de las unidades. El firewall puede bloquear las conexiones no deseadas. Sin embargo, dado que se puede estar pasando por una unidad de la empresa esta podría pasar el firewall sin problemas. Lo anterior puede convertirse en un ataque *DoS* causando una sobrecarga en el servidor (*overload*), haciendo que el sistema no esté disponible y por lo tanto ocasionando pérdida de información. Además, puede tener consecuencias sobre la confiabilidad de los datos de la empresa dado que el agente externo puede ingresar información falsa y/o alterando la misma información de la base de datos.

   - **Espionaje:** Así como se dijo anteriormente las comunicaciones se hacer a través de red celular, este tipo de comunicación es bastante sensible a ser interceptada por un tercero, si esta no está cifrada la información se expone directamente, de tal manera

que puede ser inspeccionada de forma constante (*Eavesdropping*) con el fin de robar información de la empresa o de los paquetes. Todo esto con fines maliciosos.

Propuesta de Soluciones

Mecanismos de resolución para vulnerabilidades.

Vulnerabilidad sobre la red celular	
Problema que soluciona	La intermediación de un agente externo en el canal es un factor difícil de controlar. Sin embargo, dado que esto no se puede evitar, se puede proteger la información encriptándola. Sin embargo, como se requiere que esto se procese rápidamente, se realizará bajo un algoritmo que no requiera de mucha capacidad computacional, que sea rápido pero que si sea seguro para el medio.
Participantes	Celular (Unidad) – Servidor
Tipo de Cifrado	*Cyphered-Block Chaining (CBC)*
Costo	**Bajo:** El cifrado *CBC*, es rápido por lo que no es costoso en ejecución
Eficacia	**Medio:** El algoritmo cumple con su cometido de encriptar, sin embargo, puede ser vulnerado
Eficiencia	**Alta:** Logra encriptar de manera rápida y sin consumir muchos recursos
Flexibilidad	**Alta:** Dado que es un algoritmo que no tiene una complejidad alta, es fácilmente susceptible a cambios.
Implementación	**Baja:** Es un algoritmo de fácil implementación tanto para la unidad como para el servidor.

Suplantación	
Problema que soluciona	Dado que una unidad no está autenticada, un agente externo puede incurrir en suplantación. Esto se puede solucionar con un sistema de autenticación con certificado digital.
Participantes	Celular (Unidad) – Servidor
Tipo de Cifrado	*Certificados Digitales*

Costo	**Medio:** Se requiere validar el certificado que no haya sido alterado ni la información asociada a él
Eficacia	**Alta:** Logra asegurar que la entidad que está enviando la información sea parte del sistema
Eficiencia	**Media:** Asegura que la información enviada sea de una fuente confiable. Sin embargo, tiene un costo computacional extra
Flexibilidad	**Media:** El sistema debe realizar la verificación del certificado digital antes de realizar cualquier operación. La unidad debe enviar todas sus consultas con ese certificado. Tiene un impacto en cómo interactúa el sistema, pero no afecta en gran escala al mismo
Implementación	**Media:** Se debe enviar todas las consultas desde la unidad junto con el certificado digital. Además, el servidor deberá validar el certificado.

Vulnerabilidad en los datos almacenados	
Problema que soluciona	Que un tercero pueda acceder a información confidencial ya sea de forma de lectura o escritura y que se pierdan datos dado que el espacio de almacenamiento del celular no era suficiente
Participantes	Celular (Unidad)-Servidor
Tipo de Cifrado	Electronic Code-Book (ECB)
Costo	**Bajo:** este tipo de cifrado es bastante rápido y eficiente razón por la cual no es muy costoso
Eficacia	**Medio**: Este tipo de cifrado encripta los datos que sean necesarios más puede llegar a ser descifrada su clave con los patrones que deja este tipo de cifrado
Eficiencia	**Alta:** Logra encriptar de manera rápida y sin consumir muchos recursos.
Flexibilidad	**Alta:** Dado que es la implementación del algoritmo no tiene mayor complejidad se podría cambiar sin mayor problema.
Implementación	**Baja:** Es un algoritmo de fácil implementación tanto para la unidad como para el servidor.

Espionaje	
Problema que soluciona	Un tercero desea monitorear constantemente el intercambio de paquetes que se está dando por la red celular de la compañía con el fin de conseguir información clasificada
Participantes	Celular (Unidad)-Servidor

Tipo de Cifrado	*Cyphered-Block Chaining (CBC)*
Costo	**Bajo:** El cifrado *CBC*, es rápido por lo que no es costoso en ejecución
Eficacia	**Medio:** El algoritmo cumple con su cometido de encriptar, sin embargo, puede ser vulnerado
Eficiencia	**Alta:** Logra encriptar de manera rápida y sin consumir muchos recursos
Flexibilidad	**Alta:** Dado que es un algoritmo que no tiene una complejidad alta, es fácilmente susceptible a cambios.
Implementación	**Baja:** Es un algoritmo de fácil implementación tanto para la unidad como para el servidor.